Canadian Journal of Law and Technology

Volume 15 | Number 1 Article 11

1-1-2017

The Lawful Access Fallacy: Voluntary Warrantless Disclosures, Customer Privacy, and Government Requests for Subscriber Information

Matthew P. Ponsford

The Lawful Access Fallacy: Voluntary Warrantless Disclosures, Customer Privacy, and Government Requests for Subscriber Information

Matthew P. Ponsford*

I. INTRODUCTION TO LAWFUL ACCESS IN CANADA

Lawful access to information is a broad and complex field raising significant civil rights and privacy issues for the Canadian public. The concept refers to intercepting communications and the legal authority to engage in the search and seizure of sensitive information for lawful investigative purposes. Authorities are increasingly accessing information from transmissions data or electronically intercepting telecommunication services by utilizing new *Criminal Code* powers to demand, order, and compel the preservation of electronic evidence.[1] Legislation has also expanded and streamlined the warrant process enabling authorities to intercept private communications.[2] This analysis focuses on the relationship among lawful access, customer privacy, and the publication of government requests for subscriber information. Bill C-30, introduced in 2012, and later shelved following public outcry, forms the controversial backdrop to the discussion.[3] This legislation would have "modernized" the *Criminal Code* by permitting warrantless powers over, namely, the obligatory disclosure of internet subscriber information, including one's name, address, telephone number, email address, and Internet Protocol (IP) address. The bill was widely condemned, yet unprecedented levels of warrantless requests continue. This paper explores the recent legal, political, privacy, and communications developments surrounding warrantless government requests for basic subscriber information. I assert the

---

* Matthew P. Ponsford holds a Master of Laws (LL.M.) from McGill University. He previously graduated from the Faculty of Common Law at the University of Ottawa (J.D.), completed an exchange at the Faculty of Law at the University of Hong Kong, and holds a B.Sc. (Distinction) from Queen's University. He has worked for a global law firm, several Canadian federal and provincial government departments, and public officials. He has served on the Board of Directors of several NGOs and is a member of the Canadian Bar Association. He is the sole author of nine legal journal articles, accessible via SSRN: http://ssrn.com/author=1958214.

1 *Criminal Code*, RSC 1985, c C-46 [*Criminal Code*]; *Protecting Canadians from Online Crime Act*, SC 2014, c 31 [*Online Crime Act*].

2 *Ibid*.

3 Bill C-30, *An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*, 1st Sess, 41st Parl, 2012 (first reading 14 February 2012). See also Laura Stone, "Conservatives Kill Internet Surveillance Bill C-30", *iPOLITICS* (11 February 2013), online: <www.ipolitics.ca/2013/02/11/conservatives-kill-internet-surveillance-bill-c-30> [Bill C-30].

current practice remains marred in secrecy and therefore poses a significant threat to Canadian civil liberties and privacy rights.

II. WARRANTLESS ACCESS TO BASIC SUBSCRIBER INFORMATION FOLLOWING BILL C-30

Current warrant requirements contain expanded investigative powers and reduced evidentiary burdens.[4] Few Canadians are aware of recent trends. Government agencies routinely receive warrantless access to internet subscriber information (ISI) despite the apparent illegality of the practice.[5] Canadian telecommunications service providers (TSPs) and internet companies regularly hand over ISI "hundreds of times every day"[6] and are compensated for complying with requests. Fees purportedly support the special databases companies have created to enable expeditious access by government agencies. Previously, Charmaine Borg, a Member of Parliament for the New Democratic Party, pushed for information regarding the number of requests that companies receive.[7] Companies still largely refuse to disclose that information. One government agency, the Canada Border Services Agency (CBSA), released data indicating that it made 18,849 subscriber requests in one year alone. These requests were complied with 99.9% of the time: 18,824 of 18,849, which included call records and geo-location data.[8] The CBSA paid $1–$3 compensation per request, which totalled roughly $24,211. In 2010, the RCMP similarly made over 28,000 warrantless subscriber requests.[9] This practice raises significant legal, constitutional, ethical, and privacy concerns for Canadians. Confidential ISI is still disclosed to government agencies and operatives without the knowledge or consent of people within Canada.

The development and creation of "law enforcement databases" is also disconcerting to privacy experts, yet companies continue developing improved intercept-capable transmission apparatuses to support lawful access. The paradox is that new technologies and developments are primarily being used for warrantless ISI requests. For example, the Competition Bureau acknowledged accessing Bell Canada's database 20 times in 2012–2013.[10] The "no civil or criminal liability" provision remains law for the voluntary disclosure of subscriber information, as does s. 487.0195(1), which states that no production order is necessary for peace officers or public officers' requests for voluntary

---

4 See *Online Crime Act*, *supra* note 1, s 2.

5 Michael Geist, "Internet data routinely handed over without a warrant: Geist", *Toronto Star* (28 March 2014), online: <www.thestar.com/business/tech_news/2014/03/28/internet_data_routinely_handed_over_without _a_warrant_geist.html> [Geist].

6 *Ibid.*

7 *Ibid.*

8 *Ibid.*

9 *Ibid.*

10 *Ibid.*

disclosure "that the person is not prohibited by law from disclosing."[11] The government has confronted criticisms of these provisions by stating that warrantless disclosures are permissible through exceptions found in "private sector privacy law,"[12] but it seems that it is hard to justify such wide-scale practices with significant privacy implications.

III. THE *CRIMINAL CODE* AND *R V SPENCER*: THE LEGAL FRAMEWORK

The warrantless voluntary disclosure process has typically not employed *Criminal Code* provisions as justification, namely s 487.014 (a "general production order"),[13] which can permit a justice or judge to issue an *ex parte* document production order. Around the same time Bills C-13 (lawful access) and S-4 (amending the *Personal Information Protection and Electronic Documents Act*)[14] were debated, the Supreme Court of Canada released *R v Spencer*,[15] a unanimous decision regarding the voluntary and warrantless disclosure of basic subscriber information. The Court reaffirmed internet and informational privacy, including the right to anonymity and a warrant requirement except under "exigent circumstances or where authorized by a reasonable law" and confirmed a reasonable expectation of privacy in subscriber information.[16] In the context of obtaining court orders and search warrants, although the *Online Crime Act*'s "reasonable grounds to suspect" threshold is now less stringent than the former "reasonable grounds to believe,"[17] the landmark *Spencer* decision held that obtaining subscriber information through means other than a warrant is an unlawful search and unconstitutional.

---

[11] *Online Crime Act*, *supra* note 1, s 487.0195(1). See also s 487.0195(2): "A person who preserves data or provides a document in those circumstances does not incur any criminal or civil liability for doing so."

[12] Geist, *supra* note 5.

[13] *Criminal Code*, *supra* note 1, s 487.014.

[14] See Bill C-13, *An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, 2nd Sess, 41st Parl, 2014 (assented to 9 December 2014) [Bill C-13]; Bill S-4, *An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act*, 2nd Sess, 41st Parl, 2015 (assented to 18 June 2015) [Bill S-4]. See also *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].

[15] *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212, 312 CCC (3d) 215 [*Spencer*].

[16] *Ibid* at paras 50, 62, 65–68, 71–74, quote at 71.

[17] See e.g., *Online Crime Act*, *supra* note 1; *Criminal Code, supra* note 1, ss 487.017(2),(3) as it appeared and was in force until December 9, 2014; Forms 5.004, 5.007. See also Halsbury's Laws of Canada, *Communications* (Markham, Ont: LexisNexis Canada, 2014) at HCS-107 "Lawful Access to Information" (2014 Reissue).

IV. OFFICE OF THE PRIVACY COMMISSIONER AND *PIPEDA*: THE PRIVACY CONCERNS

The Office of the Privacy Commissioner (OPC) has stated that IP addresses are *personal information* if connected to *identifiable individuals*,[18] in addition to customer names and physical addresses, especially in the internet context. Anonymous information can easily be linked to identifiable users.[19] Sections 5 to 7 of *PIPEDA*[20] outline the protection of personal information relevant to private organizations such as telecommunications service providers (TSPs) and internet companies. Section 5(3) states that an "organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[21] Bulk government voluntary disclosure requests are not consistent with this principle.

Section 7(3) outlines permissible grounds for disclosure of personal information without knowledge or consent.[22] Section 7(3)(c) permits disclosure if the company is "required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records."[23] Section 7(3)(c.1) is another option. Compliance requires government institutions to identify its *lawful authority* and indicate the purposes for obtaining information: for reasons of national security, Canadian defence, or international affairs (s 7(3)(c.1)(i)); for the purpose of enforcing Canadian law or domestic/foreign investigations relating to same, including intelligence gathering (s 7(3)(c.1)(ii)); or to administer Canadian or provincial laws (s 7(3)(c.1)(iii)). Moreover, in specific instances, TSPs and internet companies can initiate disclosure with regards to contraventions of Canadian law, national security, or victims of financial abuse.[24] Current disclosure requests are, presumably, government-initiated. Absent companies or customers verifying "lawful authority" disclosures, government institutions may continue to violate Canadian privacy legislation.

Interestingly, a proposed "lawful authority" provision contained in Bill C-12 (2011) was removed prior to the enactment of Bill S-4 (2015).[25] The original text contained pros and cons: the previous provision added specificity and clarity

---

[18] Office of the Privacy Commissioner of Canada, "Metadata and Privacy: A Technical and Legal Overview" (30 October 2014), online: < https://www.priv.gc.ca/information/research-recherche/2014/md_201410_e.pdf > at 6-7.

[19] *Spencer*, *supra* note 15 at paras 13-20.

[20] *PIPEDA*, *supra* note 14, ss 5-7.

[21] *Ibid*, s 5(3).

[22] *Ibid*, s 7(3)(a)–(i).

[23] *Ibid*, s 7(3)(c).

[24] *Ibid*, s 7(3)(c.1), (d), (d.3).

[25] Bill C-12, *An Act to amend the Personal Information Protection and Electronic Documents Act*, 1st Sess, 41st Parl, 2011 (last stage completed: first reading) [Bill C-12].

(i.e., s 3.1(*a*) "lawful authority refers to. . .") while the provision also stipulated at s 3.1(*b*) that "the organization that discloses the personal information is not required to verify the validity of the lawful authority identified by the government institution or the part of a government institution."[26] Bill S-4 was adopted in 2015 and lawful authority remains undefined. The term was implied to mean lawful authority other than a subpoena, warrant, or order, by a court, person or body, and outside the rules of court necessitating records production. The omission of the term entirely is a significant oversight.[27] I suggest future legislative amendment should include explicit mention and greater certainty of what constitutes "lawful authority" to complement *Spencer*'s interpretation of the term.

Finally, the *Canadian Charter of Rights and Freedoms* does not explicitly mention personal information protection or privacy; however, s 7 ("the right to life, liberty and security of person") and s 8 ("the right to be secure against unreasonable search and seizure") also offer protection in instances of unlawful access to subscriber information.[28] There are strong grounds for constitutional challenges against various government agencies as well as class-action lawsuits.

V. TRANSPARENCY REPORTS: DISCLOSURE PUBLICATIONS FROM TSPs AND GOVERNMENT

The reporting of voluntary warrantless disclosures presents a two-prong transparency challenge: the first is the need for more transparency regarding the number of government requests for subscriber information, and the second is the need for telecommunications to publicize the frequency of disclosures to governments. In 2011, the Office of the Privacy Commissioner (OPC) submitted requests to 14 companies inquiring about the frequency in which they were asked to share customers' data with law enforcement. Nine companies provided data aggregating 1.2 million requests, approximately 3,290 per day (2011). Several companies pooled their request numbers together to avoid further investigation, which contributed to the OPC secretly withholding data for three years (since December 2011).[29] At the time, Bill Abbott, who was Bell Canada's senior counsel and privacy ombudsman stated:

> We are walking a delicate line between supporting privacy and not antagonizing (the federal department of) Public Safety/LEAs (law enforcement agencies) so the materials will be pretty factual, not much commentary.[30]

---

[26] *Ibid*, s (3.1)(*b*).

[27] *Ibid*, s (3.1)(*a*)(i)–(ii).

[28] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the Canada *Act, 1982* (UK), 1982, c 11 [*Charter*].

[29] Alex Boutilier, "Telecom Giants Worried about 'Antagonizing' Feds on Lawful Access: Documents", *Toronto Star* (21 May 2014), online: <www.thestar.com/news/canada/2014/05/21/telecom_giants_worried_about_ antagonizing_feds_on_lawful_access_documents.html>.

The OPC claimed to have made numerous requests to telecom companies regarding government snooping, yet the same office approved the companies' "aggregation of data" strategy. Bell Canada stated it was only contacted once by the OPC and wanted legal advice and specific guidance on what they could disclose. Rogers raised similar concerns of no precedent or guidance for the request(s).[31] This is one area where ISPs and TSPs do raise valid concerns. Aggregation of data to the OPC partially resulted from uncertainty, but public relations concerns were and are a serious risk-management incentive. Rogers, TELUS and TekSavvy were among the first TSPs to release transparency reports, followed by SaskTel, MTS Allstream and Wind Mobile.[32] As of 2014, Bell Canada and Shaw Communications refused.[33] Rogers received 174,917 requests in 2013[34] and 113,655 in 2014[35]; it is uncertain how many requests the company satisfied. In 2013, Telus received 103,462 law enforcement and government requests for customer information, but refused to disclose how many requests it complied with. Telus called for an "industry-wide" reporting standard.[36] Data from 2013 suggests a 1:72 "ratio of requests to customers" for Rogers and 1:120 for Telus.[37] Both Rogers and Telus promised to publish the number of requests complied with in future reports since "its systems were not set up to track that information at the time."[38] Historical controversies could be swept under the rug without continued public pressure.

Critics argue the OPC is complicit in contested warrantless requests and not fully utilizing its regulatory powers. The sheer number of requests is shocking but relatively meaningless without more information about which, and how often, government and law enforcement agencies were and are requesting customer information. Many Canadians are unaware of this pervasive problem. Although the voluntary disclosure in response to government requests for information do not require warrants under new laws,[39] the practice sharply conflicts with

---

30 *Ibid.*

31 *Ibid.*

32 Amber Hildebrandt, "Police Asked Telcos for Client Data in Over 80% of Criminal Probes", *Canadian Broadcasting Corporation* (*CBC*) *News* (10 April 2015), online: <www.cbc.ca/news/technology/police-asked-telcos-for-client-data-in-over-80-of-criminal-probes-1.3025055>.

33 Christine Dobby, "Telus joins transparency push by sharing demands for customer info", *The Globe and Mail* (18 September 2014), online: <www.theglobeandmail.com/report-on-business/telus-joins-transparency-push-by-sharing-fed-demands-for-customer-info/article20650829> [Dobby].

34 *Ibid.*

35 Rogers, *2014 Rogers Transparency Report*, online: <www.rogers.com/consumer/privacy-crtc>.

36 Dobby, *supra* note 33.

37 *Ibid.*

38 *Ibid.*

39 *Online Crime Act*, *supra* note 1.

Spencer, which ruled warrants are required in most cases where subscriber information is sought. I suggest developing and implementing similar protocols to *PIPEDA*'s privacy breach disclosure requirements for private companies. This would add an additional safeguard for the public's privacy in the context of voluntary disclosures.

Similar issues are being adjudicated in the context of cell phone data. In the 2016 case of *R v Rogers*,[40] Justice Sproat refused a sweeping police search warrant request, which would have provided authorities with information about 40,000 Rogers and Telus customers. Telus described the police request as the most extensive demand ever received.[41] The decision highlights the important relationship between law enforcement agencies and the telecommunications sector as the gatekeeper to extensive public information. Following *Spencer*, many TSPs and internet companies adjusted their policies to require warrants and court orders from government agencies prior to granting basic subscriber information, such as customer names and address checks, yet law enforcement and government agency policies have not kept pace with private sector developments. In fact, in addition to diminished transparency from government, agencies such as Public Safety Canada are placing restrictions on private companies to *prevent the publication of private sector transparency reports*. Canadians deserve more accountability from their government.

In June, 2015, Industry Canada (reorganized as Innovation, Science and Economic Development Canada under Prime Minister Justin Trudeau) published *Transparency Reporting Guidelines*, which included guidance for "voluntary disclosures at the request of a government organization."[42] Meaningful multi-stakeholder consultations did not take place.[43] The initiative is criticized because companies are not compelled to produce reports — instead, it relies on "corporate generosity" — nor are they required to expand subscriber notification or disclose compensation tariffs.[44] The government has also failed to update its own reporting. One suggestion is for Parliament to amend the *Criminal Code*, requiring "government agencies to record and publicly report on their use of non-interception modes of surveillance."[45]

---

[40] *R v Rogers Communications Partnership*, 2016 ONSC 70, 2016 CarswellOnt 442, 128 OR (3d) 692 (SCJ) at para 42 (testing the constitutionality of "tower dumps") [*R v Rogers*].

[41] Mike Crawley, "Police sweeps of cellphone records violate privacy rights, judge rules", *CBC News* (14 January 2016), online: <www.cbc.ca/news/canada/toronto/cellphone-privacy-ruling-1.3403550>.

[42] Government of Canada, *Transparency Reporting Guidelines*, (2015) Industry Canada (now Innovation, Science and Economic Development Canada), online: <www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/transparency-reporting-guidelines-2015.pdf/$file/transparency-reporting-guidelines-2015.pdf>.

[43] Christopher Parsons, "Industry Canada Transparency Report Guidelines Intensely Problematic", Telecom Transparency Project (30 June 2015), online: <www.telecomtransparency.org/industry-canada-transparency-report-guidelines-intensely-problematic>.

[44] *Ibid.*

Although most companies have adjusted their policies, it is unclear if and how many are still granting warrantless access to authorities. Indeed, depending on the company, there is a patchwork of practices and inconsistent application of voluntary disclosure rules. And further, "the fact that Internet providers may have revealed such information in the past does not provide a compelling reason to eliminate the critical safeguards provided by the warrant process."[46] Additionally, if and when warrantless voluntary disclosures are sought, information is likely inadmissible in legal proceedings since it constitutes an illegal search.

VI. CONCLUSION AND RECOMMENDATIONS

The judiciary and civil society serve important functions since each ensures that government power is curbed. Although law enforcement and security agencies demand new powers — asserting barriers to obtaining subscriber information "expeditiously" — the claims are largely unsubstantiated. Law enforcement should bear the onus and burden of proof to demonstrate how current laws impede investigations.

Parliament enacted *PIPEDA* to strike a balance between privacy rights and cybercrime, and instructed ISPs to respect court orders and judicial oversight. A Department of Justice discussion paper circulated to federal, provincial, and territorial cybercrime working groups proposed three legislative options to obtain basic subscriber information, and purportedly complying with *Spencer*: (1) an administrative scheme without court approval; (2) modifications or redesign to the judicial order process, and (3) a subscriber information request process with a heightened expectation of privacy through a judicial court process and a non-judicial, administrative procedure for "less sensitive subscriber data."[47] Expanding warrantless access to voluntary disclosures of personal information is inconsistent with the *Charter*. In January, 2016, the OPC urged Parliament "to confirm the Spencer principles and clarify the very narrow scope of circumstances in which law enforcement can obtain subscriber information without a warrant."[48]

Unfortunately, lawsuits arising from privacy violations by private institutions and government are rarely successful in Canada in comparison to the United States (U.S.). This is due to the limited powers of the Privacy

---

[45] *Ibid.*

[46] Michael Geist, "What Now? Privacy and Surveillance in Canada After the Paris Attacks" (27 November 2015), *Michael Geist* (blog), online: <www.michaelgeist.ca/2015/11/what-now-privacy-and-surveillance-in-canada-after-the-paris-attacks>.

[47] Jim Bronskill, "RCMP Need Warrantless Access to Online Subscriber Info: Paulson" *CBC News* (26 November 2015), online: <www.cbc.ca/news/politics/paulson-rcmp-subscriber-info-warrantless-access-1.3337028>.

[48] Daniel Therrien, "Op-ed: Federal Privacy Commissioner Urges Caution Should Parliament Revisit Warrantless Access", *OPC News* (25 January 2016), online: <www.priv.gc.ca/media/nr-c/2016/oped_160125_e.asp>.

Commissioner of Canada who cannot make binding orders without evidence or impose financial penalties for non-compliance.[49] Other jurisdictions possess markedly "more robust enforcement powers" such as significant administrative monetary penalties.[50] For example, the U.S. Federal Trade Commissioner negotiates high-profile financial settlements regarding privacy breaches. Order-making powers for data protection authorities also exist in the United Kingdom, New Zealand, Ireland, and Spain.[51] These jurisdictions offer excellent examples of effective public policy. Canada should integrate these countries' systems and processes while adapting the scheme to suit its specific needs. We must ensure that there is an adequate balance between the privacy of Canadians and human rights objectives while reserving warrantless options for matters of public safety and national security in very precise circumstances.

The OPC continues to lack effective oversight surrounding this issue. Although the two most controversial elements contained in Bill C-30 were removed — warrantless mandatory basic subscriber information disclosure, and requirements for telecom companies to develop intercept capability — the government continues operating outside the law, often compensating companies for their intercept capability systems. There are lawful and expeditious ways to obtain basic subscriber information through judicial oversight. It is unclear what other revelations could surface in coming years, and whether all companies and government agencies remain compliant with *Spencer*'s principles.

In the interim, the federal government could order an impartial investigation into its practice of obtaining subscriber information. Regardless, judicial oversight, industry guidance, and legislative overhaul are urgently required. Internet providers and TSPs have not committed publicly to notify customers of government requests for data. Improved telecommunications transparency reporting also requires Innovation, Science and Economic Development Canada to initiate a multi-stakeholder consultation process and address its flawed guidelines. Furthermore, future legislation could include transparency requirements for: (1) an annual government report detailing voluntary disclosure request data across all departments and agencies, and (2) the notification to specific subscribers when their informational privacy is infringed. Without the revision of far-reaching government practices that lack judicial oversight, "lawful access" is indeed a fallacy, and it is one that invades the individual privacy of the Canadian public.

---

[49] Ian Munroe, "Bell Data Collection Part of 'Disturbing Trend'", *CBC News* (30 October 2013), online: <www.cbc.ca/news/technology/bell-data-collection-part-of-disturbing-trend-1.2223949>.

[50] *Ibid.*

[51] Office of the Privacy Commissioner, "The Case for Reforming the *Personal Information Protection and Electronic Documents Act*" (May 2013), online: <www.priv.gc.ca/parl/2013/pipeda_r_201305_e.pdf> at 6.